GETTING STARTED FOR VENDORS

Step	✓	Procedure
1		Review the WAWF Vendor Guide and Quick Reference Guide
2		Set Up an Electronic Business Point of Contact (EB POC) in CCR
3		Activate CAGE Code and Establish a Group
4		* Optional Step* Designate a Group Administrator Manager (GAM)
5		* Optional Step* Establish an Organizational E-Mail Address
6		Determine if Batch Feeds for Data Input are Necessary
7		Set up your Computer
8		Self-Register Online starting with the GAM
9		Change Password
10		Practice Entering Invoices in WAWF Training Site

1. **Review the WAWF Vendor Guide and Quick Reference Guide.**

2. **Determine who is designated as the Electronic Business Point of Contact (EB POC) in the government's Central Contracting Registry (CCR) database for your company. The Electronic Business POC is the only authorized representative for your company to activate your vendor profile in WAWF.** Your company may have up to two EB POC's listed for each CAGE Code. To view your company's CCR profile, you can search the database on your vendor CAGE Code at www.ccr.gov by clicking the "Search CCR" link.

   To update your CCR account, please contact CCR Assistance Center at 888-227-2423 or 616-961-4725.

   Adding or Changing an EB POC in the CCR Database
   - Go to www.ccr.gov and click the Update or Renew Registration Using TPIN option on the left hand side.
   - Enter your DUNS number and TPIN code.
   - Go to the left hand side of the web page and select Points of Contact. When that page comes up, scroll down to the Electronic Business Point of Contact fields. Enter the information and hit the validate/save button.

3. **The EB POC must submit a request to establish a Group in WAWF for your company. This step must be accomplished before you can register for a WAWF Login ID.** Some companies with multiple locations may have more than one CAGE Code set up in a hierarchy structure, but most vendors will have just one CAGE Code. To establish a group for your CAGE Code in WAWF, the EB POC must call the WAWF Customer Support Center at the phone number listed on the WAWF home page 1-866-618-5988, or send and email requesting CAGE Code activation in WAWF (please include "WAWF" in the subject line) to cscassig@ogden.disa.mil including the name of your company and the CAGE Code(s). If you need immediate access to WAWF, please call rather than emailing your request. The phone activation will take approximately five minutes.

4. **Decide how many users will be accessing WAWF and designate a Group Administrator (OPTIONAL STEP).** All vendor WAWF users will be able to select roles of "Vendor", "Vendor View-Only", or "Group Administrator" when they self-register. Users may also have multiple roles. Vendors with more than one person accessing WAWF should appoint at least one Group Administrator (GAM) to manage and activate users in the vendor's organization to have access to WAWF data. The GAM may be the same person designated as the EB POC. Each GAM must submit an official "appointment letter" signed by the EB POC. The signed appointment letter should be faxed to 703-991-0455. (See sample GAM appointment letter at the end of these instructions).

***Note:** If the GAM is the same person as the EB POC, the GAM letter is **not required**. When registering for WAWF, a GAM must select the Vendor role and the Group Administrator role. The Group Administrator's manual is available for reviewing to all WAWF registered users. The GAM manual can be found in the Software Users Manual link within the WAWF application after logging into WAWF.*

5. **Establish an Organizational E-Mail Address (OPTIONAL STEP).** WAWF-RA routes information according to the CAGE Codes. The electronic documents themselves do not get routed, but status notifications about the documents are sent via e-mails. For example, e-mail confirmations are sent when a vendor SUBMITS a document. E-mail notifications are sent when the government ACCEPTS or REJECTS the document. In order to receive status information about the WAWF documents, vendors need to establish an organizational email address and determine who will have access to the organizational email. The e-mail address may be a "distribution group" address, set up by the vendor's e-mail administrator, which may be sent to multiple users on the vendor's side, for example, "wawf@companyname.com". Ensure that the organizational e-mail address is operational and can receive e-mails prior to registering it with the WAWF Customer Support Center. The GAM can change the organizational email address at any time.

   ***Note:** If you do not set up an organizational e-mail address, the e-mail address of the first individual that self-registers from your CAGE/DUNS code will be used as the default organizational e-mail address. If you are the only one submitting invoices through WAWF, you can use your own email address.*

6. **Determine if batch feeds for data input is necessary (OPTIONAL STEP)**. Vendors should submit documents via the File Transfer Protocol (FTP) or Electronic Data Interchange (EDI) process if they have a large number of transactions and/or many line items per transaction. The WAWF-RA FTP and EDI Guides are available after the vendor's account has been activated. If further assistance is needed, contact the WAWF-RA Customer Service Center at 1-866-618-5988, a Joint Interoperability Test Center (JITC) technician will assist in testing your file layout(s).

   ***Note:** You will need to fill out DD Form 2875* and fax to WAWF PMO at 703-991-0455.

7. **Set up the software on your computer.** Each computer will need software set up as specified under the "Setting Up Your Machine" link on the WAWF home page. Most likely, your computer is already set up and configured properly to be able to use WAWF. If you have an in-house systems administrator who controls software on your machine, contact them for assistance. Otherwise, please follow the steps below.

   - Go to the WAWF website https://wawf.eb.mil/.
   - Click the link in the left column "About WAWF-RA".
   - Click on the sub link for "Setting Up Your Machine".
   - Perform steps 1-6 (skip steps 4 and 7 for Digital Certificates) to complete PC set-up and configuration.

   Minimum System Requirements:

   - Microsoft Windows 98, Windows NT 4.0 SP6a, Windows 2000, or Windows XP
   - Internet Explorer (128 bit) Version 5.5 SP2 or later *or* Netscape Navigator (128 bit) 4.76, 4.78, or 4.79. *If you have an older version of IE, Microsoft offers free downloads to upgrade to version 6.0 from their website.*
   - Adobe Acrobat Reader 4.0 or later. *Free to download.*

8. **Have all WAWF users complete WAWF Self-Registration Online, starting with the GAM.** Users can self-register anytime after a group has been established in WAWF for your CAGE Code by the EB POC and system requirements have been met. Directions for the Self

Registration process are also located on the WAWF production home page under the "Help" link in the center of the WAWF home page.

On-line Self-Registration Procedures:

- Using your web browser open the WAWF production web site https://wawf.eb.mil/ and click on the 'Self Register' link.
- Once on the registration page, fill in the mandatory fields, "First Name," "Last Name," "Commercial Phone," "Email address," "Job Description," and "Title."
- Select the radio button labeled User ID and Password.
- Type in a User ID, which must be 8 characters long minimum (create your own).
- In the "Role" drop down menu, choose "Vendor."
- In the CAGE Code field, type your Cage code. Do not put anything in the "extension" field. (Your CAGE code must already be activated by WAWF Customer Support.)
- When a security message appears, click "Yes".
- Review the information you have entered. You may click on the icon to edit the information.
- Additional Step for GAMs: In the "Role Information" section, under the "Action" column, click the icon to add a role (looks like file cards). In the drop down box choose "Group Administrator" and click continue. Enter your CAGE code in the "Group Name" field. Click the OK button when the security box appears.
- Finally, if everything on the screen is correct, click on the check box for "Statement of Accountability" and hit the "Register Now" button (you must submit the form for it to be valid).

***Note:** Vendor users may register to access WAWF-RA with either a User ID/Password combination or an external certificate. We recommend vendors register with a User ID/Password to get started using WAWF. Vendors who want to purchase a PKI certificate may buy them from one of three sources. Please visit the "registration help" link on the home page to find out how.*

9. **Please change your password.** All users will receive an email from WAWF–DISA Ogden Customer Support within 48 hours following his or her self-registration with a one-time temporary password. If you do not receive an email with a temporary password, please call WAWF Customer Support at 1-866-618-5988. All users will be directed to change their one-time passwords the first time they log into WAWF, after which they may begin using WAWF.

10. **Practice entering invoices in WAWF Training Site.**
Follow the detailed instructions in the Vendor Guide or Vendor Quick Reference Guide to create an invoice. We recommend that you practice entering an invoice in the WAWF training site (https://wawftraining.eb.mil/) before using the production site.

***Note:** There is a demo login and password listed on the web page for the test site, along with demo CAGE Codes and DoDAAC numbers. When entering data in WAWF, be certain to TAB between fields. If documentation needs to be attached to the invoice in WAWF (i.e.: proof of delivery documents, contractor timesheets, or line item detail not included in the WAWF line items) please prepare or scan the attachment prior to initiating the WAWF invoice.*

The DoDAAC numbers for your real invoices in the production database will be based on your contract. You will need to obtain the following DoDAACs from your contract and/or your Government Contracting Officer:

- Issuing Office DoDAAC
- Admin Office DoDAAC
- Inspector DoDAAC *(may not be required for your contract)*
- Acceptor/Ship To DoDAAC

- LPO DoDAAC *(Certifying Office)*
- Pay Office DoDAAC

For questions regarding computer set-up and login activation, please contact the WAWF help desk at 1-866-618-5988 or cscassig@ogden.disa.mil.

For questions regarding your contract and WAWF invoicing terms or DoDAAC number information, please contact your Navy contracting officer or the NAVY WAWF Assistance Line at 1-800-559-WAWF.

Helpful web sites:

WAWF home page:
https://wawf.eb.mil

Web based training:
http://www.wawftraining.com

WAWF test site:
https://wawftraining.eb.mil

DFAS E-invoice payment information for processed invoices:
http://www.dfas.mil/money/vendor (under Non-MOCAS System, click on a query type)

Note: Cut and paste onto Company Letterhead & fax to WAWF PMO 703-991-0455

Sample Appointment Letter
For Designating Group Administrators

[Enter the Group Administrator Manager's name]
[Enter the Group Administrator Manager's email address]
[Enter the Group Administrator Manager's phone number]

1. You are hereby appointed a (primary OR alternate) Group Administrator for the WAWF application. Your span of control includes the following CAGE codes. [Type in or attach list]

2. You are responsible for the following activities:
   a. Establish hierarchical sub-groups for managing user accounts, as necessary.
   b. Establish organizational e-mail for each CAGE and submit these to the Ogden Customer Service Center at 1-866-618-5988, or via e-mail (cscassig@ogden.disa.mil, include WAWF in subject line)
   c. Instruct registrants within your span of control to register.
   d. Activate and update users in your group within one business day of request.
   e. Ensure that requests for user access are valid and assign access at the appropriate authorization and privilege level.
   f. Ensure that subordinate group administrators and alternates are created, as necessary.

3. As a group administrator, you are a critical part of maintaining system security because you have the ability to grant access to users. You are responsible for validating the "need to know" of the users that you activate, and would be responsible for de-activating an invalid user. Ensure that users are who they say they are and that only the privileges necessary to accomplish their job duties are associated with this activated user account.

4. If a user's account needs to be de-activated, you are responsible for de-activating that account by following the procedure in the Group Administrator Manual (GAM).

EP POC Signature Block
Email Address
Phone Number

Note: Group Administration Manual will be received after the Group Administrator has been established.

SYSTEM AUTHORIZATION ACCESS REQUEST (SAAR)

PRIVACY ACT STATEMENT

AUTHORITY: Executive Order 10450, 9397; and Public Law 99-474, the Computer Fraud and Abuse Act.

PRINCIPAL PURPOSE: To record names, signatures, and Social Security Numbers for the purpose of validating the trustworthiness of individuals requesting access to Department of Defense (DoD) systems and information. NOTE: Records may be maintained in both electronic and/or paper form.

ROUTINE USES: None.

DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information may impede, delay or prevent further processing of this request.

TYPE OF REQUEST □ INITIAL □ MODIFICATION □ DELETION □ USER ID ________________	DATE
SYSTEM NAME *(Platform or Applications)*	LOCATION *(Physical Location of System)*

PART I *(To be completed by Requestor)*

1. NAME *(Last, First, Middle Initial)*		2. SOCIAL SECURITY NUMBER
3. ORGANIZATION	4. OFFICE SYMBOL/DEPARTMENT	5. PHONE *(DSN or Commercial)*
6. OFFICIAL E-MAIL ADDRESS	7. JOB TITLE AND GRADE/RANK	
8. OFFICIAL MAILING ADDRESS	9. CITIZENSHIP	10. DESIGNATION OF PERSON

USER AGREEMENT *(Complete Block 29 or 30 as appropriate)*

I accept the responsibility for the information and DoD system to which I am granted access and will not exceed my authorized level of system access. I understand that my access may be revoked or terminated for non-compliance with DISA/DoD security policies. I accept responsibility to safeguard the information contained in these systems from unauthorized or inadvertent modification, disclosure, destruction, and use. I understand and accept that my use of the system may be monitored as part of managing the system, protecting against unauthorized access and verifying security problems. I agree to notify the appropriate organization that issued my account(s) when access is no longer required.

IA TRAINING AND AWARENESS CERTIFICATION REQUIREMENTS *(Complete as required for user or functional level access.)*

□ I have completed Annual Information Awareness Training. DATE ________________

11. USER SIGNATURE	12. DATE

PART II - ENDORSEMENT OF ACCESS BY INFORMATION OWNER, USER SUPERVISOR OR GOVERNMENT SPONSOR *(If individual is a contractor - provide company name, contract number, and date of contract expiration in Block 16.)*

13. JUSTIFICATION FOR ACCESS

14. TYPE OF ACCESS REQUIRED:
□ AUTHORIZED □ PRIVILEGED LEVEL OF CERTIFICATION CLEARANCE ________________

15. USER REQUIRES ACCESS TO: □ UNCLASSIFIED □ CLASSIFIED *(Specify category)*
□ OTHER ________________

16. VERIFICATION OF NEED TO KNOW I certify that this user requires access as requested. □	16a. EXPIRATION DATE FOR ACCESS *(Specify date if less than 1 year)*

17. SUPERVISOR'S NAME *(Print Name)*	18. SUPERVISOR'S SIGNATURE	19. DATE
20. SUPERVISOR'S ORGANIZATION/DEPARTMENT	20a. SUPERVISOR'S E-MAIL ADDRESS	20b. PHONE NUMBER
21. SIGNATURE OF INFORMATION OWNER/OPR	21a. PHONE NUMBER	21b. DATE

22. SIGNATURE OF IAO	23. ORGANIZATION/DEPARTMENT	24. PHONE NUMBER	25. DATE

26. SYSTEM ADMINISTRATOR:
I have completed my Annual Requirement for Information Assurance awareness.

□ YES □ NO DATE ________________

Reset

27. OPTIONAL INFORMATION

PART III - SECURITY MANAGER VALIDATES THE BACKGROUND INVESTIGATION OR CLEARANCE INFORMATION

28. TYPE OF INVESTIGATION	28a. CLEARANCE LEVEL

28b. IT LEVEL DESIGNATION	28c. DATE	28d. TYPE OF DESIGNATION
29. VERIFIED BY *(Print name)*	30. SIGNATURE	31. DATE

PART IV - COMPLETION BY AUTHORIZED STAFF PREPARING ACCOUNT INFORMATION

TITLE:	SYSTEM	ACCOUNT CODE
	DOMAIN	
	SERVER	
	APPLICATION	
	DIRECTORIES	
	FILES	
	DATASETS	
DATE PROCESSED	PROCESSED BY *(Print name and sign)*	DATE
DATE REVALIDATED	REVALIDATED BY *(Print name and sign)*	DATE

Reset

INSTRUCTIONS

A. PART I: The following information is provided by the user when establishing or modifying their USER ID.

(1) Name. The last name, first name, and middle initial of the user.

(2) Social Security Number. The social security number of user.

(3) Organization. The user's current organization (i.e. DISA, SDI, DoD and government agency or commercial firm).

(4) Office Symbol/Department. The office symbol within the current organization (i.e. SDI).

(5) Telephone Number/DSN. The Defense Switching Network (DSN) phone number of the user. If DSN is unavailable, indicate commercial number.

(6)Official E-mail Address. The user's official e-mail address.

(7) Job Title/Grade/Rank. The civilian job title (Example: Systems Analyst, GS-14, Pay Clerk, GS-5)/military rank (COL, United States Army, CMSgt, USAF) or "CONT" if user is a contractor.

(8) Official Mailing Address. The user's official mailing address.

(9) Citizenship. The user's citizenship status.

(10) Designation of Person.

IA Training and Awareness Certification Requirements. User must indicate if he/she has completed the Annual Information Awareness Training and the date.

(11) User's Signature. User must sign the DD Form X455 with the understanding that they are responsible and accountable for their password and access to the system(s).

(12) Date. The date that the user signs the form.

B. PART II: The information below requires the endorsement from the user's Supervisor or the GovernmentSsponsor.

(13). Justification for Access. A brief statement is required to justify establishment of an initial USER ID. Provide appropriate information if the USER ID or access to the current USER ID is modified.

(14) Type of Access Required: Place an "X" in the appropriate box. (Authorized - Individual with normal access. Privileged - Those with privilege to amend or change system configuration, parameters, or settings.)

(15) User Requires Access To: Place an "X" in the appropriate box. Specify category.

(16) Verification of Need to Know. To verify that the user requires access as requested.

(16a) Expiration Date for Access. The user must specify expiration date if less than 1 year.

(17) Supervisor's Name (Print Name). The supervisor or representative prints his/her name to indicate that the above information has been verified and that access is required.

(18) Supervisor's Signature. Supervisor's signature is required by the endorser or his/her representative.

(19) Date. Date supervisor signs the form.

(20) Supervisor's Organization/Department. Supervisor's organization and department.

(20a) E-mail Address. Supervisor's e-mail address.

(20b) Phone Number. Supervisor's telephone number.

(21) Signature of Information Owner/OPR. Signature of the functional appointee responsible for approving access to the system being requested.

(21a) Phone Number. Functional appointee telephone number.

(21b) Date. The date the functional appointee signs the DD Form X455.

(22) Signature of IAO. Signature of the IAO or sponsoring office responsible for approving access to the system being requested.

(23) Organization/Department. IAO's organization and department.

(24) Phone Number. IAO's telephone number.

(25) Date. The date IAO signs the DD Form X455.

(26) System Administrator. Place an "X" in the appropriate box and indicate date Information Assurance requirement was completed.

(27) Optional Information. This item is intended to add site specific information, as required.

C. PART III: Certification of Background Investigation or Clearance.

(28) Type of Investigation. The user's last type of background investigation (i.e., NAC, NACI, or SSBI).

(28a) Clearance Level. The user's current security clearance level (Secret, Top Secret).

(28b) IT Level Designation. The user's ADP designation (ADP1, ADP3, etc.).

(28c) Date. Date of last investigation.

(28d) Type of Designation. The user's last ADP designation (ADP1, ADP2, etc.).

(29) Verified By. The Security Manager or representative prints his/her name to indicate that the above clearance and investigation information has been verified.

(30) Signature. The Security Manager or representative signature indicates that the above clearance and investigation information has been verified.

(31) Date. The date that the form was signed by the Security Manager or his/her representative.

D. PART IV: This information is site specific and can be customized by either the DoD, functional activity, or the customer with approval of the DoD. This information will specifically identify the access required by the user.

E. DISPOSITION OF FORM:

TRANSMISSION: Form may be electronically transmitted, faxed, or mailed. Adding a password to this form makes it a minimum of "FOR OFFICIAL USE ONLY" and must be protected as such.

FILING: Original SAAR, with original signatures in Parts I, II, and III, must be maintained on file for one year after termination of user's account. File may be maintained by the DoD or by the Customer's IAO. Recommend file be maintained by IAO adding the user to the system.